Transition Plan

For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

Prepared By:
MDA Systems Ltd.
Suite 60, 1000 Windmill Road
Dartmouth NS B3B 1L7

MDA Reference # DN0773, Issue 1/1
Contract Project Manager: Brett Trask, 902-481-3511
PWGSC Contract Number: W7714-040875/001/SV
CSA: Marc Gregoire, Technical Authority, 613-998-2113

Contract Report

November 2009

DRDC-RDDC-2014-C111

Principal Author

Original signed by Brett Trask

Brett Trask

Project Manager, JNDMS

Approved by

Approved for release by

Abstract

In today's modern warfare environment the ability to conduct Network Enabled Operations has become crucial to the success of any military organization. This dependence on the networks and the information superiority that they provide has heightened the requirement to understand how networks may be vulnerable and to defend against cyber threats that may attempt to exploit these vulnerabilities. The Joint Network Defence and Management System (JNDMS) Technology Demonstrator (TD) has successfully demonstrated the value of combining the domains of enterprise network management with network security management to provide comprehensive Situational Awareness (SA) for Computer Network Defence (CND) to the Canadian Forces. Through numerous experiments and demonstrations, culminating with the demonstration of a full system deployment on the Defence Research Experimental Network, the project has shown that the costs, risks and complexities of engineering such a system can be greatly reduced by the integration of currently available Commercial off the Shelf (COTS) products into a flexible, open standards-based system architecture.

The final activity for the JNDMS TD is to illustrate a path to operations that describes a feasible approach for evolving the Technology Demonstration System to a full implementation on the DND networks. This report contains recommendations which will greatly reduce the risk and associated costs of following this path.

A great deal of effort during the JNDMS TD has been focused on mitigating the risks involved with transitioning the demonstration system to a fully operational deployment. The development and inclusion of key artifacts in this report such as a thorough Concept of Operations, a System Requirement Specification including Certification and Accreditation steps, and a comprehensive Deployment Strategy with costs will demonstrate the user that the JNDMS is a valid and well-planned base-option for providing the Canadian Forces with an advanced Network Defence Capability.

Résumé

Dans l'environnement de guerre moderne, pouvoir mener des opérations facilitées par réseaux (OFR) est devenu un facteur vital à la réussite de toute armée. Cette dépendance sur les réseaux et la supériorité de l'information qu'ils rendent possibles a souligné l'importance de comprendre comment les réseaux peuvent être vulnérables et comment les défendre contre les cybermenaces qui pourraient essayer d'exploiter ces vulnérabilités. Le démonstrateur de technologies (DT) du Système interarmées de défense et de gestion des réseaux (SIDGR) a réussi à démontrer la valeur pour les Forces canadiennes de marier la gestion des réseaux d'entreprise et la gestion de la sécurité des réseaux afin de permettre la connaissance de la situation en matière de défense des réseaux informatiques. Ce projet a démontré par de nombreuses expériences et démonstrations (conclues par la démonstration du déploiement d'un système complet sur le réseau expérimental de recherches en défense, DREnet) qu'il est possible de réduire considérablement le coût, les risques et la complexité d'élaborer un tel système en intégrant des logiciels commerciaux standards pour créer une architecture souple et fondée sur des normes ouvertes.

La dernière activité du DT SIDGR vise à montrer la voie vers des opérations qui décrivent une stratégie pragmatique visant à faire avancer le système démonstrateur de technologies vers sa mise en œuvre complète sur les réseaux du MDN. Le présent rapport renferme des recommandations qui réduiront considérablement les risques et les coûts associés à cette stratégie.

Nous avons consacré de gros efforts, au cours de la conception du DT SIDGR, à atténuer les risques associés au passage d'un système de démonstration à un déploiement pleinement opérationnel. L'élaboration et l'inclusion dans le présent rapport d'éléments importants, comme un concept opérationnel exhaustif, les spécifications liées aux exigences du système (notamment les étapes d'homologation et d'accréditation et une stratégie de déploiement complète accompagnée des coûts associés) démontreront à l'utilisateur que le SIDGR constitue une option de base valide et bien conçue visant à munir les Forces canadiennes d'une capacité de défense du réseau évoluée.

Executive summary

Transition Plan: For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

Brett Trask; November 2009.

The Joint Network Defence and Management System (JNDMS) Technology Demonstrator (TD) was developed from the beginning with a strong emphasis on not only proving that there is a need for Situational Awareness (SA) for Computer Network Defence (CND), but to also investigate and make practical recommendations for the transition of the TD system towards an operational deployment for the Canadian Forces. To this end, a significant effort was expended to ensure that the development efforts included the creation and maintenance all of the engineering artefacts typically associated with the development of a production system. By doing this, the JNDMS has been able to successfully demonstrate over three distinct development cycles and a live network deployment that many of the hurdles and risks associated with an operational implementation of the JNDMS on Department of National Defence (DND) networks have been resolved and ultimately documented in this report.

The JNDMS was designed from the beginning to consolidate the domains of Network Enterprise Management and Information Technology (IT) Security management to greatly simplify the job of DND's IT Network Security Analysts. By also presenting this data in the context of military operations, the system provides Operational Command with a situational picture that describes the health of the IT infrastructure on which an operation depends and the current risks facing that infrastructure from numerous cyber threats. This Situational Awareness now allows Operational Commanders to manage and protect their key information assets as they would more traditional military assets.

In designing the JNDMS, the project team concentrated on developing a system architecture that would be both flexible and scalable, ensuring that any further investment by DND would result in a capability would remain relevant over many years and that would scale along with the implementation of new COTS applications, network services and the growth of DND networks. In order to accomplish this, the design team ensured that a great deal of modularity was built into the JNDMS, with interfaces between the architecture components that are based on commonly accepted industry standards. The other key to the JNDMS architecture is the employment of commercial grade enterprise COTS. By integrating the COTS with loosely coupled, standards-based interfaces, the JNDMS receives the benefits of providing large amounts of functionality, but also the ability to integrate new or replacement COTS products with very little engineering effort.

A key artefact in the deployment of any mission critical system and its adoption by operators is a thorough Concept of Operations (ConOps). Through consultation with the Security Analysts and Network Engineers at the Canadian Network Operations Center (CFNOC), as well as, key Subject Matter Experts within the Canadian Forces Information Operations Group (CFIOG), the JNDMS project team has included in this report a ConOps that describes the key considerations for the system's deployment to operations on both the CLASSIFIED and Designated domains.

Another important component of the transition to operations for the JNDMS is a detailed Deployed System Requirements Specification. During the development of the JNDMS and especially during deployments at the Coalition Warrior Interoperability Demonstrations (CWID) 2007 and the final deployment for experiments and demonstrations on the Defence Research Experimentation Network (DREnet), the project team was able to work through and document many of the considerations necessary to successfully deploy on DND networks. The Specification described within this report discusses key requirements such as: description of the scope of the deployment, security considerations including key elements for certification and accreditation such as a Statement of Sensitivity and Threat/Risk Assessment, as well as important performance considerations to which the system must adhere.

Also developed and included in the report is a Deployment Strategy which describes the actual work plan and schedule, the products that would need to be purchased, and integrated and the cost of the deployment for the recommended scope. This and the following sections describe the recommended level of testing and integrated logistics support for the system provides the detail necessary for DND to compare the JNDMS with other commercially available options for SA for CND. All components of this strategy incorporate and benefit from many years of documented systems integration experience contained within the project team; specifically with DND as the customer.

Finally the report discusses the assumptions and challenges that the team has been able to identify as requiring resolution prior to a complete deployment of the JNDMS to the DND networks. The majority of the assumptions are based on tools that the project may not have to provide as they or a similar capability that JNDMS would leverage may be already owned by DND at the time of a JNDMS deployment.

Overall the JNDMS has, by virtue of meeting all of the stated project requirements, met its goal of developing an SA for CND system that will be of high value to the Canadian Forces Network Operations Centre (CFNOC). This Transition to Operations Report further demonstrates that the JNDMS is a viable option to provide the Canadian Forces with a robust capability for Network Defence Command and Control.

Sommaire

Transition Plan: For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

Brett Trask; Novembre 2009.

Dès le départ, nous avons mis au point le Démonstrateur de technologies (DT), Système interarmées de défense et de gestion des réseaux (SIDGR) dans le but non seulement de prouver l'existence d'un besoin pour connaître la situation en défense des réseaux informatiques, mais aussi d'étudier et de formuler des recommandations visant la transition du système de DT vers son déploiement opérationnel au sein des Forces canadiennes. À ces fins, nous avons consacré au cours de l'élaboration des efforts importants à la rédaction et la tenue à jour de tous les éléments d'ingénierie habituellement associés aux systèmes destinés au déploiement opérationnel. Le SIDGR a ainsi pu démontrer, au cours de trois cycles de développement distincts et d'un déploiement sur un réseau opérationnel, que bien des écueils et des risques associés à la mise en place opérationnelle du SIDGR sur les réseaux du ministère de la Défense nationale ont été résolus puis en dernier lieu exposés dans le présent rapport.

Le SIDGR a été conçu dés le départ dans le but de combiner les domaines de gestion des réseaux d'entreprise et de gestion de la sécurité des technologies de l'information (TI) afin de simplifier considérablement le travail des analystes de la sécurité des réseaux des TI du MDN. En présentant aussi ces données dans le contexte des opérations militaires, le système donne au commandement opérationnel une vision de la situation qui décrit l'état de l'infrastructure des TI sur laquelle dépend une opération et les risques actuels que présentent nombre de cybermenaces pour cette infrastructure. La connaissance de la situation permet maintenant aux commandants des opérations de gérer et de protéger leurs biens d'information importants comme ils peuvent actuellement le faire avec les biens militaires habituels.

Pour concevoir le SIDGR, l'équipe du projet a axé ses efforts sur l'élaboration d'une architecture de système souple et évolutive. On assure ainsi que tout investissement subséquent du MDN entraînera une capacité qui restera utile de nombreuses années et qui pourra évoluer en parallèle tant avec la mise en œuvre de nouvelles applications commerciales et de nouveaux services réseau qu'avec la croissance des réseaux du MDN. Pour atteindre cet objectif, l'équipe de conception a donné au SIDGR une architecture hautement modulaire; les interfaces entre les diverses composantes sont fondées sur des normes communes de l'industrie. L'autre facteur clé de l'architecture du SIDGR, c'est l'utilisation de logiciels standards commerciaux. L'intégration de logiciels commerciaux et d'interfaces faiblement couplées mais normalisées donne au SIDGR une vaste gamme de fonctions, mais aussi la capacité de remplacer ou d'ajouter des logiciels commerciaux sans trop d'efforts en ingénierie.

Un concept opérationnel (ConOps) exhaustif est essentiel au déploiement de tout système essentiel à la mission et de son adoption par ses utilisateurs. Après des consultations avec les analystes en sécurité et les ingénieurs réseau du Centre d'opérations de réseaux des Forces canadiennes (CORFC) et avec divers experts en la matière du Groupe des opérations d'information des Forces canadiennes (GOIFC) l'équipe du projet SIDGR a pu intégrer au présent

rapport un ConOps qui expose les points importants entourant le déploiement opérationnel de ce système dans les domaines CLASSIFIÉ et désigné.

Les spécifications détaillées des exigences du système déployé constituent un autre élément important de la transition du SIDGR vers un système opérationnel. L'équipe du projet a pu, au cours de ses travaux d'élaboration du SIDGR et particulièrement lors des déploiements en vue des expériences et des démonstrations sur le réseau expérimental de recherches en défense (DREnet), explorer et documenter un grand nombre des facteurs requis pour le déployer sur les réseaux du MDN. Les spécifications que renferme le présent rapport traitent des exigences les plus importantes : une description de la portée du déploiement; les questions de sécurité, notamment les éléments clés nécessaires à l'homologation et à l'accréditation, comme l'énoncé de sensibilité et l'évaluation de la menace et des risques; ainsi que des normes importantes de rendement que le système doit respecter.

L'équipe a aussi élaboré une stratégie de déploiement, intégrée au présent rapport, qui décrit le plan de travail et l'échéancier réels, les produits qu'il faudrait acheter et intégrer et le coût du déploiement pour la portée recommandée. Cette section et la suivante décrivent les activités d'essai et le soutien logistique intégré recommandés pour ce système de façon suffisamment détaillée pour permettre au MDN de comparer le SIDGR avec les autres options de connaissance de la situation disponibles commercialement au Canada. Tous les éléments de cette stratégie intègrent et exploitent les nombreuses années d'expérience éprouvée en intégration de systèmes, particulièrement pour le MDN, acquises par les divers membres de l'équipe.

En dernier lieu, le présent rapport traite des hypothèses et des questions qui aux yeux de l'équipe doivent être résolues avant de déployer le SIDGR à grande échelle sur les réseaux du MDN. La plupart de ces hypothèses sont fondées sur des outils que le projet n'aura peut-être pas à fournir; si le MDN les possède (ou possède des outils équivalents) au déploiement du SIDGR, il pourra en tirer parti.

En gros, le SIDGR a respecté toutes les exigences du projet et atteint l'objectif d'élaborer une capacité de connaissance de la situation pour les systèmes canadiens qui sera extrêmement utile au Centre d'opérations des réseaux des Forces canadiennes (CORFC). Le présent rapport de transition au milieu opérationnel démontre en outre que le SIDGR constitue un moyen viable de fournir aux Forces canadiennes une capacité robuste de commandement et contrôle de défense du réseau.

Table of contents

List of figures

List of tables

This page intentionally left blank.

1 Introduction

The Joint Network Defence and Management System (JNDMS) Transition To Operations Report is intended to serve as a "way-ahead" in transitioning the JNDMS System as delivered at the end of the JNDMS TD to a fully operational system providing Situational Awareness for Computer Network Defence to the Department of National Defence.

At the point of completion for the JNDMS TD, the JNDMS will, by virtue of achieving the stated project requirements, comprise an SA for CND system that will be of high value to the Canadian Forces Network Operations Centre (CFNOC). In order to make the leap from successful technology demonstration to a fully operational system, the JNDMS will require a period of transition that has associated non-recurring engineering, costs and numerous challenges and considerations.

This plan will provide a blueprint for the transition of the JNDMS including descriptions of further development effort, cost estimates, recommended schedule and duration, as well as technical requirements, challenges, assumptions and proposed solutions.

2 Applicable Documents

This document makes reference to a number of existing documents that are required for in-depth context for topics presented in this report:

- System Requirements Specification for the Joint Network Defence and Management Project DID SD 001
- Architectural Design Document for the Joint Network Defence and Management Project DID SD 002
- Test Design Document for the Joint Network Defence and Management Project DID SD 003
- Design Document for the Joint Network Defence and Management Project DID SD 004
- Project Management Plan for the Joint Network Defence and Management Project DID PM 001
- Department of National Defence/Canadian Forces Information Certification and Accreditation Guideline, Version 1.4, December 2006
- Harmonized Threat and Risk Assessment (TRA), TRA-1 October 23, 2007 – developed by IT Security Client Services, Communication Security Establishment

3 JNDMS TD Background

3.1 Overview

The JNDMS Technology Demonstration (TD) project was intended to extend the research into Situational Awareness for Computer Network Defence conducted by the Network Information Operations Section of DRDC Ottawa. In meeting the System Requirements Specification for the JNDMS, the Integrated Project Team (IPT) was able to engineer a functioning Proof of Concept (POC) System, which has served to validate the potential and feasibility of such a system to provide a much-needed Information Operations capability to the Canadian Forces Network Operations Centre (CFNOC).

The JNDMS was designed for the specific purpose of extending Canada's capability in network defence and management. In addition to the management and protection of DND's operational networks, Military Commanders require the ability to assess the health and availability of the networks and network services in the same way that they would for any other operational asset, such as a ship, a tank, or plane. The JNDMS project was developed on the concept that knowledge of an IT asset's purpose and how an operation depends on it are key information elements required by Operational Command.

The role of enterprise management tools and security management tools are well entrenched in network management today. The role of these systems and their best practices are captured in best practices and standards processes such as the Information Technology Infrastructure Library (ITIL). One of the goals in the development of JNDMS was to leverage these tools and best practices where possible and to build on top of Commercial-Off -The Shelf (COTS) tools. The JNDMS IPT was keenly aware that the scope and resources available to any commercial offering would overshadow this project and would improve over time. It was therefore beneficial to make use of these tools where possible.

Over the duration of the project and after an extensive Design effort, the JNDMS was developed over 3 distinct development cycles, each with specific objectives. More detail on each of the development cycles may be found in the JNDMS Project Management Plan DID PM-001. Formal demonstrations of the system at each stage of development were conducted for members of the DND community and members of Other Government Departments (OGD) with similar cyber-defence interests. Of particular interest, the IPT was fortunate enough to demonstrate the JNDMS at the end of the second development cycle through participation in the Coalition Warrior Interoperability Demonstrations (CWID) 2007.

Finally, the JNDMS TD was able to meet another key objective through the deployment of the system on a live operational network. The initial phases of the project were deemed sufficiently successful to warrant an extension to deploy the system to the DRDC experimental network. The deployment served to validate the scalability of the developed solution, as well as to provide further evidence to DND of the value of achieving robust Situational Awareness for Computer Network Defence.

3.2 TD System Architecture

The JNDMS TD has developed an architecture containing specific system components that define the implementation of the JNDMS, as shown in Figure 1. Each of these components has required interfaces and system processes. Each of the system components provide standard interfaces that allow them to interact with other components. The implementation of these standard interfaces also allows the JNDMS to remain extremely scalable and flexible with regards to the specific components and COTS products that may require integration in any operational implementation of the system.

For the purposes of this report, only the high level system architecture components are described. Further detail into the JNDMS Architecture may be found in the Architectural Design Document for the JNDMS, DID SD 002.

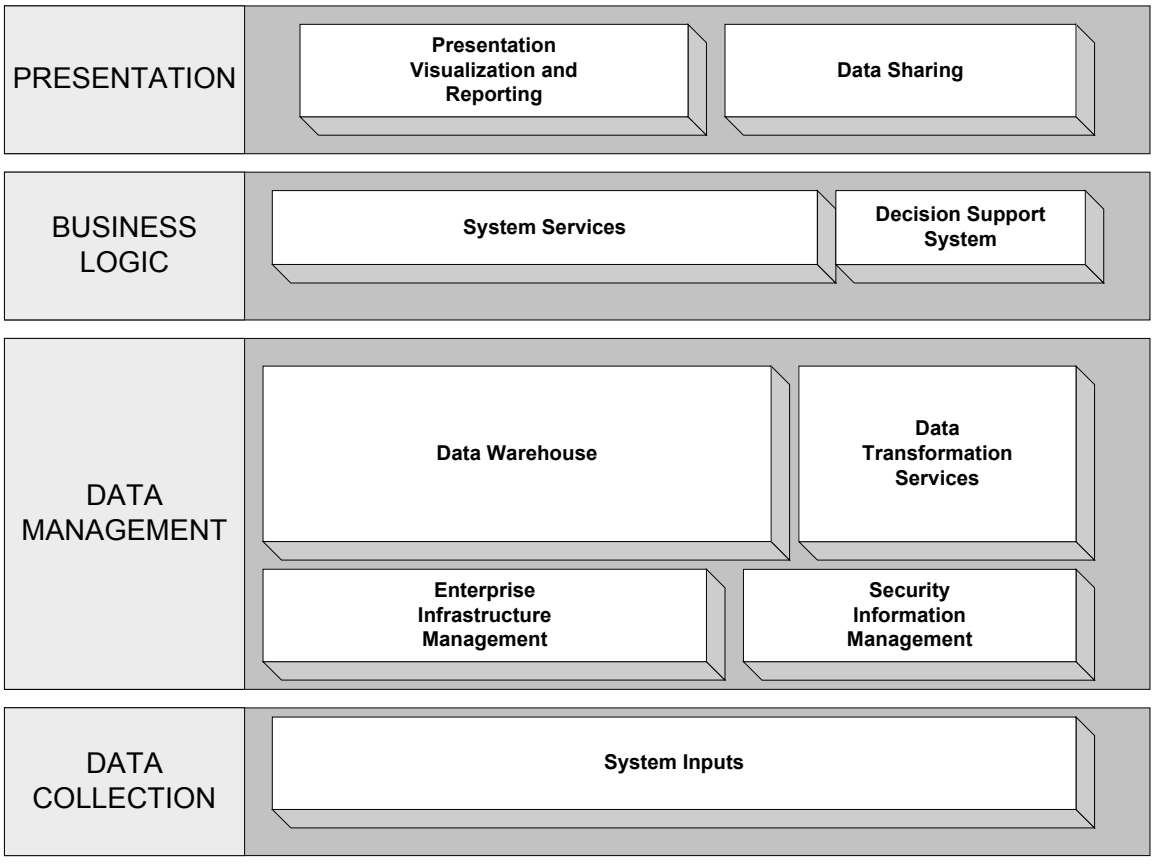

Figure 1: High-Level Systems Architecture of the JNDMS

The JNDMS high-level architecture is composed of the following:

- Data Collection Components

  The JNDMS leverages established Commercial Off-The-Shelf (COTS) or open-source products to perform some of the more challenging aspects of CND data acquisition. They include Security Information Management (SIM) products, Enterprise Infrastructure Management (EIM) products, Host Vulnerability Scanners, and Network Infrastructure Discovery and Mapping products. The role of JNDMS is to integrate and manage the results of these tools, and not to replicate similar functionality.

- Data Management Components

  DND is a security conscious organization and as a result employs a great deal of security-point products, which generate large volumes of security event data. The SIM component performs initial data fusion and correlation processing on security event data and only injects qualified security events, as well as other interesting security related events into the JNDMS. EIM and Data Collection components also perform some level of data fusion and correlation processing.

  The JNDMS stores all its data, whether acquired or created, in the JNDMS Data Warehouse. The JNDMS Data Warehouse is implemented with a COTS relational database management system (RDBMS). COTS RDBMS products include the necessary features to achieve data integrity, data replication and data backup. When in persistent storage, JNDMS data maintains contextual attributes, such as temporal, origin, and severity attributes.

- Business Logic Components

  A core component of the JNDMS is the JNDMS System Services (JSS) that is responsible for initial pre-processing, system I/O, coordination with the Decision Support System (DSS) and tasks related to data model integrity.

  The JNDMS Decision Support System (DSS) is responsible for the analysis of incoming events. This component maintains internal state machines that can identify the current status of the system, including topology and dependency information. This component may, optionally, use a business rules management system to augment its analysis.

- Presentation Components

  JNDMS includes state-of-the-art visualization technology to convey SA information in highly contextual forms. The JNDMS presentation component supports role-based interactions with the JNDMS operator. Network administrators require the most detailed information, while network and security analysts mandate information pertinent to incidents. Finally, Military Commanders simply demand to know how incidents affect their missions. The JNDMS presentation component provides the correct information to the correct operator at the appropriate time.

The JNDMS also includes mechanisms to permit sharing of SA data with JNDMS installations in the same security domain, with JNDMS installations in other security domains, as well as the information assurance systems of coalition partners. Information sharing policies and information sharing agreements control the flow of shared SA data both in (import) and out (export) of the JNDMS. A solution has also been implemented to permit information sharing between networks of different security classifications using one-way communication devices commonly referred to as data-diodes.

4 System Concept of Operations

The JNDMS is intended to provide an enhanced capability to the Canadian Forces through a more automated and centralized flow of information for computer network defence. The information presented by the JNDMS is in some cases unavailable to CFNOC staff, or at the very least is currently provided by a number of disparate systems and processes requiring a large number of personnel organized into separate cells. The separation of these cells has fostered the growth of stove-piped systems and processes, reporting to the Watch Officer and to the NO&S. The JNDMS will provide the opportunity for an improved work-flow, allowing for the streamlining of the CFNOC staff and making the sharing of information and reporting much more efficient. It must be noted that the JNDMS IPT understanding of the CFNOC roles and responsibility structure is based on analysis performed during the early part of 2006. This document assumes that the structure has evolved over time but that the JNDMS will still offer opportunities to further streamline and improve the overall workflow for the CFNOC team.

4.1 Role

The JNDMS is an information system that provides a rich interface for the presentation of Situational Awareness (SA) Picture for Computer Network Defence (CND). The primary system users are the staff members of the CFNOC, including Network Analysts, IT Security Analysts and Information Operations Commanders. The JNDMS provides information contextualised for each of these groups in an integrated single portal interface that facilitates both a robust high-level view of the networks' defensive posture as well as the detailed views of the information required for Analysts to fully understand the core of any issues, outages or cyber-threat that may arise. The sensitivity of the information processed and generated depends on the specific network to which the system is deployed. For example, on the designated network, the JNDMS is configured to gather, but not necessarily correlate the information gathered and will therefore only generate information at up to a Protected A classification. However, when that data is passed to the Classified domain, where it is correlated, possibly with data gathered at the Classified domain, the information processed and generated must be treated as up to SECRET.

4.2 Locations

The primary user base for the JNDMS is the staff of the CFNOC located at Canadian Forces Station Leitrim. The systems at this facility will be used by the NO&S, Watch Officer and members of the Service Desk, Critical Incident Response Team and Network Vulnerability Assessment Team. The CFNOC will require two installations of the JNDMS for the Canadian Secret Network Infrastructure (CSNI) and one on the Defence Wide Area Network (DWAN). Each of the JNDMS installations currently resides on six rack mount servers comparable to the HP ProLiant DL380. Although not a core JNDMS component, the system will require to interface with a DND deployed PKI server to provide the necessary level of user access control.

The rational for having two installations on the CSNI is that one installation will reside at the CFNOC and the other will reside at another location, providing redundancy at the operational level, at which the JNDMS provides the most comprehensive SA. In the event of the loss of installations at CFS Leitrim, the offsite JNDMS on the CSNI will be available instantly, while the installation on the DWAN can be restored from back-ups and hardware spares. The systems on the CSNI require identical configurations and in turn, require identical Security Certification and Accreditation as the primary systems.

As the JNDMS is a complex system that contains a significant DND owned codebase that integrates a large number of data interfaces to COTS systems, a test and development environment will each be required. The test and development environments will each require, as a minimum, two full JNDMS installations. The test environment must be identical to the operational systems and the development environment must be sufficiently similar to the test and operational installations to allow for the operation and further development of the most current operational system version.

4.3 Operational Authority

The Operational Authority for the JNDMS system and applications is the Commanding Officer of the CFNOC. The Operational Authority will have ownership of the system and responsibility for it employment and is expected to provide direction in the evolution of the system to continue to meet its stated objectives.

A designated System Manager will be responsible for the deployment, access control functional use, maintenance of the JNDMS. The System Manager must also either assume the responsibility for or manage the interface to the appointed Life Cycle Management team. The Life Cycle Management of the JNDMS will include application, database and hardware functions and will also be required to manage any National Data Server replication functions.

4.4 Target System Architecture

The JNDMS is a distributed application that implements principles of Service Oriented Architecture and Standard Interfaces. Detailed architecture information may be found in the JNDMS Architecture Design Document DID SD 002.

At a high level, the JNDMS architecture consists of four key levels: Data Collection, Data Management, Business Logic and Presentation.

The JNDMS Data Collection Layer facilitates the key system inputs that include Enterprise Information Management (EIM), IT Security data and Military Operations data. The EIM and IT Security data come primarily via commercially available COTS. Military Operations data current comes in the form of user-entered forms provided by the JNDMS, but the system has been constructed such that operations data can come via an automated interface in the future.

The Data Management Layer consists primarily of the JNDMS Data Warehouse and Data Transformation Services. The data warehouse is an Enterprise Oracle RDBMS and the data transformation services. These services transform the data from their source format and move the data into data warehouse. To accomplish this task a large variety of transformation technologies are provided via standard interfaces including XML, ODBC, JDBC, CORBA and SNMP.

The Business Layer in JNDMS has been titled the JNDMS System Services (JSS) and is consisting of Java programs constructed following the Java 2 Enterprise Edition (J2EE) standard. The primary function of the JSS is to process the raw data within the JNDMS to implement the Decision Support System functionality.

Finally the Presentation Layer of the JNDMS consists of a rich featured web-portal User Interface. The portal has been implemented with the Google Earth Web Toolkit. It is important to note that in order for the JNDMS portal to function properly, the system must have access to one of DND's licensed Google Earth Enterprise Servers (see assumptions section of this document).

Specific functional components and interfaces between them have been identified as the high-level architecture for the JNDMS.

4.5 User Access Control

JNDMS users must have a valid user ID and password to access a specific instance of the JNDMS using the workstation common web browser on the Local Area Network (LAN) where the application exists. The JNDMS is developed to employ Entrust Certificates/Public Key Infrastructure assuming that PKI service is available on the CSNI and the DWAN.

As the JNDMS is a deployed to a LAN, users must have a valid LAN account that they will require to log in to prior to accessing the JNDMS application. The JNDMS System Manager is responsible for providing JNDMS user IDs and passwords to qualified users and will be required to maintain a list of individuals who have been granted access to the application/data servers.

User access within the application is based on specific assigned roles. Within each role the data views into the application are developed and managed by the System Manager. Also, the System Manager will grant specific roles to users that match their requirements of the system and their operational role in the organization.

4.6 Interfaces with Other Systems

The JNDMS is designed to interface with other systems on a number of different levels:

- System Inputs – the JNDMS is designed to interface with a multitude of COTS products to provide the data required to produce SA for CND. The products facilitate the gathering of information from the five identified key domains: IT infrastructure and services, military operations, vulnerabilities and exploits, safeguards and security events. For a detailed description of these systems, please refer to the JNDMS Detailed Design Document DID SD 004.

- Other JNDMS installations – the JNDMS provides the ability to interface with other JNDMS systems, either on a peer network of the same security classification, or with a JNDMS system on a higher security classification via a one-way data diode. This form of interface is accomplished with the replication feature of the Oracle RDBMS. The SA sharing interface design for the JNDMS is described in Figure 2.

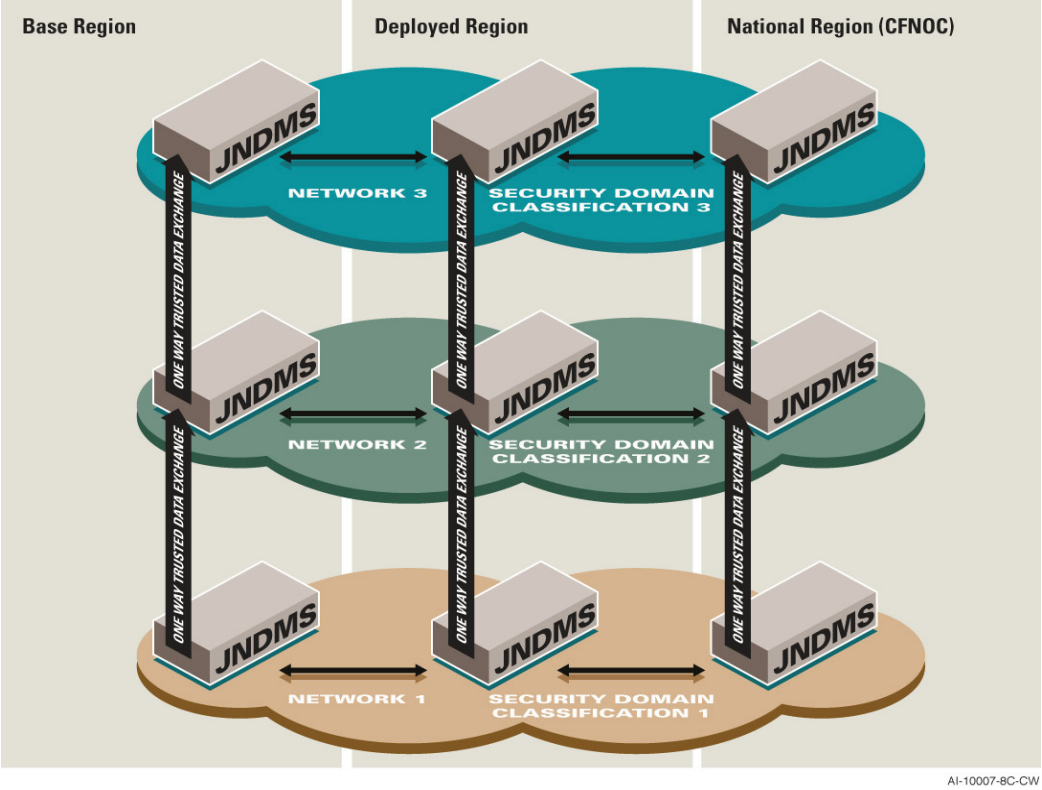

Figure 2: JNDMS Situational Awareness Data Sharing

- Google Earth Enterprise Server – the JNDMS User Interface Portal has been developed with the Google Earth Web Toolkit and the Google Earth plug-in. This component of the JNDMS requires connection to a Google Earth Enterprise Server in order to function.

- Data Sharing includes both data export and data import between different levels of security classifications.

4.7 System Security

The JNDMS being a cyber-security system, it has the capability to process and generate sensitive information and therefore requires to be handled with a number of levels of security itself. This section describes the security measures that will be required to ensure the appropriate level of information confidentiality is maintained. Further detail on the JNDMS Security Architecture may be found in the JNDMS Architecture Design DID SD002.

4.7.1 Application and Data Warehouse Security

The JNDMS application and data warehouse incorporates a number of security features to ensure the confidentiality, integrity, and availability of the data.

Access control of data is implemented through the combination of the following strategies:

- Partitioning of secure data from non-secure data, or sensitive data from non-sensitive data. This facilitates access control at the systems level.
- Implementation of user-level access control within the database management system.
- Implementation of user-level access control within the middleware for the portal application.
- Use of "peer systems profiles" to dictate what data views are synchronized to which JNDMS peers; for example one profile for a CF to CF synchronization, and another for a CF to a US Military Information Assurance System.

Encryption is used as appropriate using standards based mechanisms:

- Encapsulation of JDBC/ ODBC calls over the network using SSL or Secure Internet Profile (IPSEC) tunnelling.
- Appropriate use of on-disk encryption using encrypting file systems where host Threat Risk Assessment dictates.

Integrity checking mechanisms are built into the underlying relational database management technology and additional mechanisms, such as inclusion of calculated message digests on input files, can be included in the data schema as well.

Backup and recovery mechanisms that exist within the database technology will be leveraged both technically and through CONOPS documentation, including how and when to use full or partial restores.

Additional security can be managed through full database encryption through the use of the Oracle 11g RDBMS.

4.7.2 System Level Security

The following provides a general description of the JNDMS system level security precautions:

1. **Personnel Security**. The JNDMS user community consists of members of the CFNOC staff including Commanding Officer and Watch Officer, Service Desk Operators, CIRT and NVAT Analysts. All must have Canadian SECRET Level II Security clearances as a minimum, but access to the system should be provided by the System Manager on a "Need to Know" basis.

2. **Physical Security**. At all locations, the System resides within the confines of a military installation and is protected under the applicable local Security Orders.

3. **Procedural Security**. Information System Security Officers (ISSO) are appointed for the overall system and at each location where JNDMS IS assets are installed and the information is processed. The role of the ISSO is to provide security advice, produce and coordinate C&A documentation, to ensure that the conditions of accreditation are maintained and to respond to security direction from the overall system ISSO.

4. **Information Technology Security (ITSEC).** The following highlights individual security features of the implemented JNDMS ITSEC facets:

    a. **Computer Security (COMPUSEC).** The following lists the existing COMPUSEC features:

        i. Formal access approval is enforced. Only those individual that have a functional need to access the system's Data Servers are granted a User Name and Password by the System Manager based on their specific operational role(s).

        ii. Users can only access the JNDMS installation assigned to them by their System Manager. The System Manager can only access the JNDMS in their assigned domain.

    b. **Transmission Security (TRANSEC).** Communication with JNDMS via the CSNI requires TCP/IP and strong access control enforcing user ID and password authentication at both the network and application levels.

    c. **Network Security (NETSEC).** In order to communicate with the JNDMS, either via the application or an SQL Data Query Tool, a valid User Name and Password is required. The protection of the JNDMS topology and routing is provided by using the CSNI as its backbone. It is therefore assumed that any real threat would originate internally. To combat an internal threat the following security is applied:

        i. Strong Identification and Access control, and

        ii. Separation of user roles; JNDMS User, JNDMS Owner (Database Administrator/Schema Owner) and JNDMS Admin/System.

5 Deployed System Requirements Specification

5.1 System Specification

This section details the scope of deployment, security and performance considerations for two installations of the JNDMS on the DND CSNI and one installation of the JNDMS on the DWAN for gathering and forwarding System Inputs only. The intent of this section is to cover those aspects of a deployed JNDMS that are not already covered by the following project documents:

- System Requirements Specification for the Technology Demonstration of the Joint Network Defence and Management System (JNDMS) Project DID SD 001.
- Architectural Design Document for the Technology Demonstration of the Joint Network Defence and Management System (JNDMS) Project DID SD 002.
- Design Document for the Technology Demonstration of the Joint Network Defence and Management System (JNDMS) Project.

5.1.1 Scope

For the purposes of the Deployed System Requirements of the JNDMS, the scope of the target network(s) will be limited to two installations on the DND Classified domain, known currently as the CSNI and one installation on the designated network or DWAN. Table 1 describes the scope of the CSNI and the DWAN at the time of this writing. It is important to note that these figures are hypothetical estimates from Subject Matter Experts and not to be taken as exact figures. Figure 3 describes the software that JNDMS would interface to for various System Inputs.

Table 1: Target CSNI and DWAN Network scopes

Object	CSNI	DWAN
Assets		
- Servers	260	3,000
- Hosts	6,000	120,000
- Network Infrastructure	600	9,000
- Software		
Users	8,000	90,000
Administrators	100	5,000
Missions	26 (c1 demo)	
Locations	552 (IAT)	

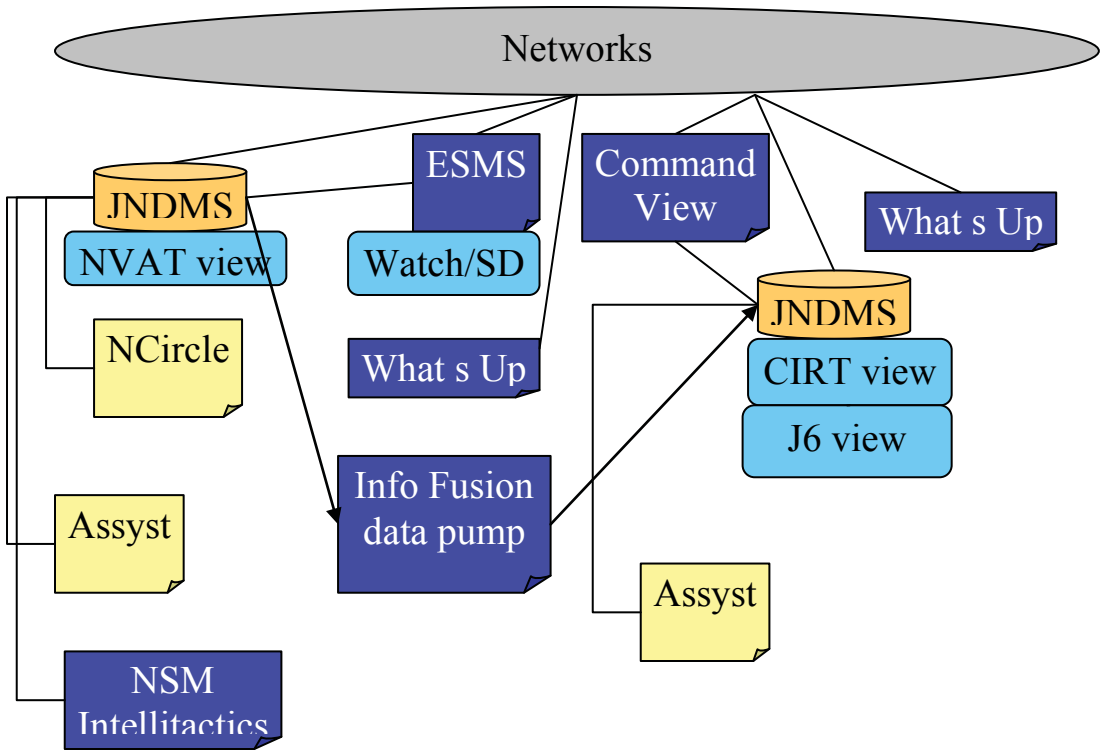

Figure 3: Target Licenses

5.2 Security Considerations

A system as complex as JNDMS with multiple installations required across security domains as well as interfaces with a large number of COTS products requires significant effort and planning in regards to security and obtaining the necessary Certification and Accreditation (C&A) required prior to deployment on DND networks. Consideration must be given to identify all System stakeholders and engage Directorate of Information Management Security (Dir IM Secur) early in the JNDMS transition to operations to ensure the smooth and comprehensive C&A process. It is important to note that the C&A process spans the duration of the life-cycle of the system and requires re-visiting and attention every time there is an update or change to the system, which includes following the DND Request For Change (RFC) process.

It is important to note that the C&A process for the JNDMS must focus on the core JNDMS system. Any of the systems that are implemented as system inputs for the JNDMS will almost certainly be COTS that must receive an independent C&A. If any of these products are introduced to DND as part of a JNDMS Transition to Operations Project, the project would also bear the responsibility for the C&A of those products.

The following section describes some of the key points of the C&A process and requirements for a DND information system. Many of the topics discussed here come directly from and may be found in the following publications:

- Department of National Defence/Canadian Forces Information Certification and Accreditation Guideline, Version 1.4, December 2006.

- Harmonized Threat and Risk Assessment (TRA), TRA-1 October 23, 2007 – developed by IT Security Client Services, Communication Security Establishment.

5.2.1 DND Certification and Accreditation Requirements

Concept of Operations

Every IT system to be deployed to a DND network will require a Concept of Operations (ConOps) that will describe among other things, the usage and intent of the system to facilitate an operational group in meeting their stated objectives. There are several key components of a ConOps that must be considered at the earliest stages of the C&A process:

- Introduction of common key security principles
- Any known constraints
- Interdependencies and relationships with other projects/systems
- The potential context or benefits of the system to the operational users
- Categories of users and function for information sensitivity and "need to know" considerations
- System Management
- System Security Policies showing that they fall within departmental security guidelines
- Security View to introduce the safeguards and security risk management solutions
- Consideration into the personnel, procedural, physical and technical security requirements (to be developed in detail during the project's development and testing phases)

Section 4 of this document provides an example of an initial Concept of Operations for a JNDMS Transition to Operations Project.

Standard Operating Procedures

Standard Operating Procedures (SOP) are considered a key procedural security safeguard for a system and are seen as key to the continuance of secure information processing with replacement staffs. For the JNDMS Transition to Operations Project a key activity of the project definition phase will be comprehensive review of the approximately 200 SOPs currently contained CFNOC "Playbook" database to ensure that necessary SOPs are implemented and/or revised in the context of the JNDMS system. This will ensure that the use of the system is beneficial and that procedures key to the secure and effective operations by the CFNOC staff remain well documented and available.

Statement of Sensitivity

The statement of Sensitivity is a key aspect of the C&A process as it is used by Dir IM Secur as the initial reference point for the level of assurance in the system's security and determines the level of effort to be considered for the accreditation of the system.

The Statement of Sensitivity also describes the most important components of the system from an information management perspective and is therefore key to the planning and development of the system TRA.

The following are the key requirements of a Statement of Sensitivity that must be documented to ensure the C&A process can move forward:

- Operational Role of the system (may be gleaned from ConOps)
- System Description including all components and may be gleaned from other more detailed project documents such as Architecture and Design
- Determination of Sensitivity based on the values of confidentiality, integrity and availability
- Injury test, which is used to determine the impact of compromised assets such as the levels of injury in general, to people both physical and psychological and finally financial impact
- Security classification required by the system, which in the case of JNDMS depends on the network to which an installation is deployed
- Asset integrity, confidentiality and availability values

The development of a Statement of Security for an Operational JNDMS Deployment Project requires a significant effort due to the fact that the system has a large number of system interfaces and the ability to process and generate extremely sensitive information about DND computer networks.

Network & System Diagrams

As previously mentioned, a detailed system description of all components of an Information System is required for the C&A process. For the JNDMS, it is anticipated that the Architectural Design, Detailed Design and System Requirements Specification Documents (DIDs SD 001, 002 and 003) provide the level of detail required for C&A.

Threat/Risk Assessment

An accurate TRA is the most important aspect of the C&A process for information system security. The TRA process is initiated by the development of the Statement of Sensitivity described in the previous section. A completed TRA provides assurance that the safeguards for a system are correct and correctly implemented. The implementation of these safeguards allows for the establishment of a System Security Baseline that must be maintained throughout the life-cycle of the system. Figure 4 describes the phases and processes recommended for a TRA project in the Harmonized Threat and Risk Assessment Methodology published by the Royal Canadian Mounted Police (RCMP) in 2007.

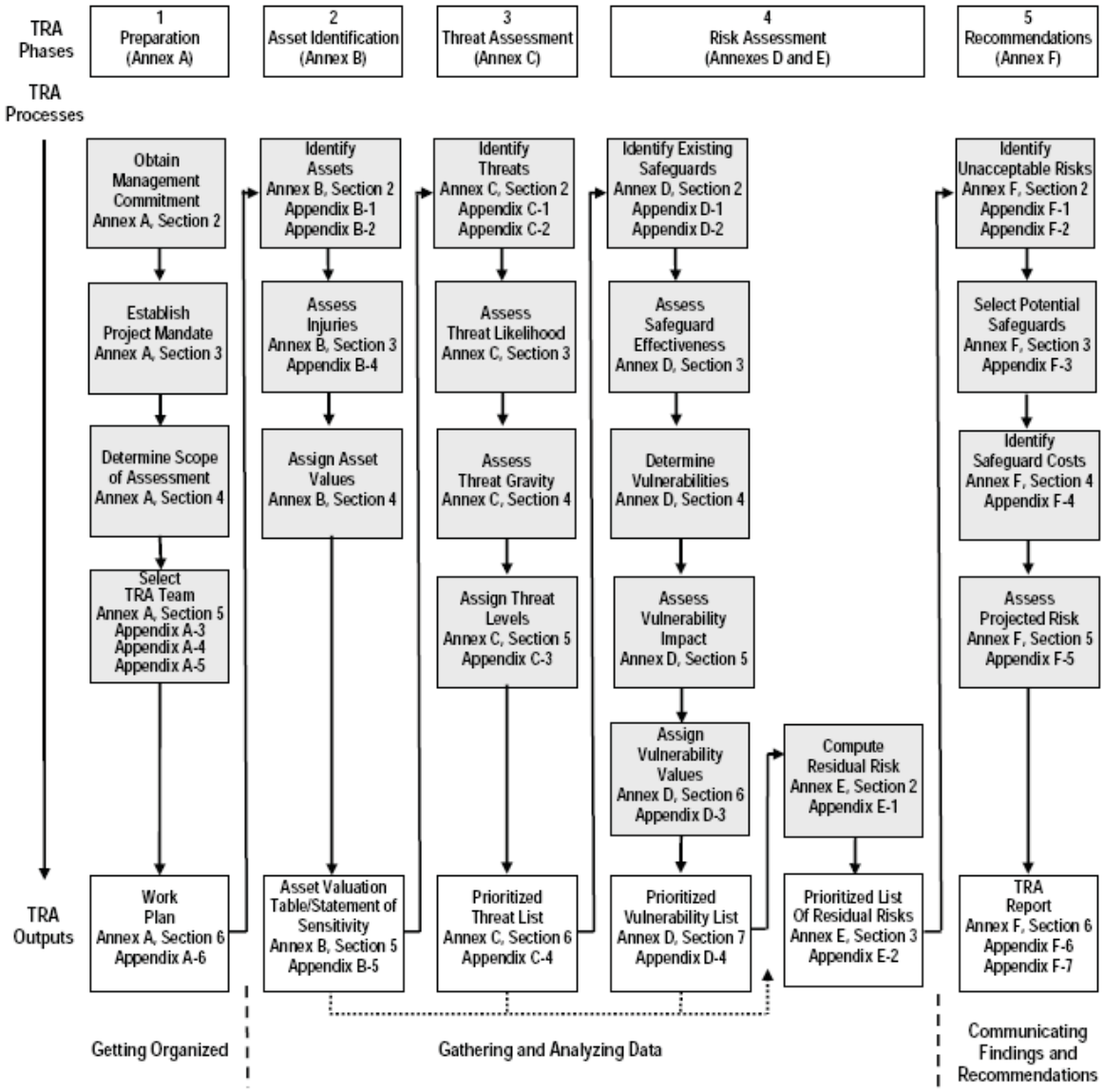

Figure 4: Phases and Processes of the HTRAM published by the RCMP in 2007

5.3 Performance Considerations

The JNDMS moves, transforms, stores, processes, and presents extremely large volumes of data. As is the expectation of a Technology Demonstration Project, a number of performance and scalability issues, both anticipated and unexpected were encountered. Many of these were mitigated and developed into the current system. Mostly due to budget and schedule constraints, a number of these were unable to be mitigated, but will require serious attention during a JNDMS Transition to Operations Project.

5.3.1 Network Bandwidth

Throughout the JNDMS Technology Demonstration, the IPT has monitored a technical risk regarding the amount of network bandwidth consumed by the system and more importantly by the COTS products required to provide core system inputs. To provide a comprehensive Situational Awareness picture, the JNDMS requires a large variety of information, including network topology and results of vulnerability scans and software inventory scans. These have shown to be the most bandwidth intensive actions required by the JNDMS and by eliminating any of these data sources, the quality and relevance of the SA JNDMS can produce is compromised.

The final phase of the JNDMS TD which saw the deployment of the JNDMS on the DREnet included the installation and configuration of several COTS systems including the CA Spectrum network management system and the nCircle IP360 vulnerability management system. By examining the bandwidth impact of these systems as witnessed during the DREnet deployment we can see that it is feasible to implement procedures to minimise the impact of these systems on network bandwidth, while providing the key inputs that JNDMS requires to produce effective SA.

The CA Spectrum system continuously monitors DREnet systems for availability. The following graph in Figure 5 shows the typical bandwidth utilized by the Spectrum system within a 24 hour period to monitor of DREnet systems. Monitoring traffic consists of Simple Network Management Protocol (SNMP) requests and responses as well as SNMP traps.

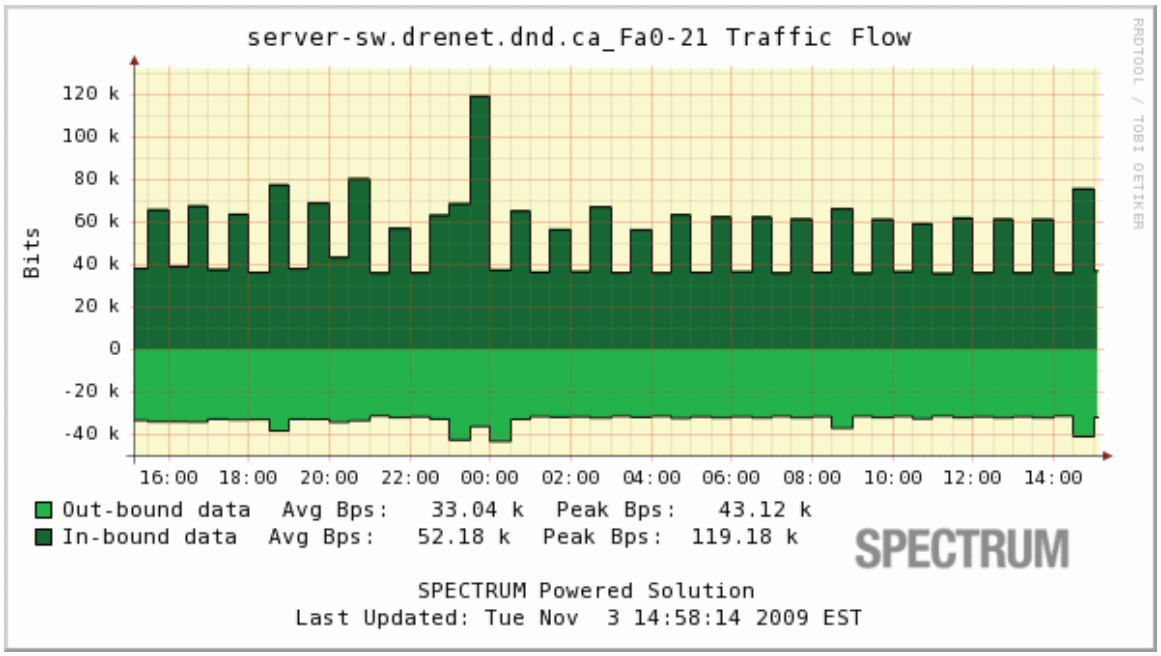

Figure 5: CA Spectrum Bandwidth Utilization over a 24 hour period

The IP360 system scans DREnet systems for vulnerabilities every night beginning at 22:00 ET. The following graph in Figure 6 shows the typical bandwidth utilized by the IP360 system within a 24 hour period to scan DREnet systems.

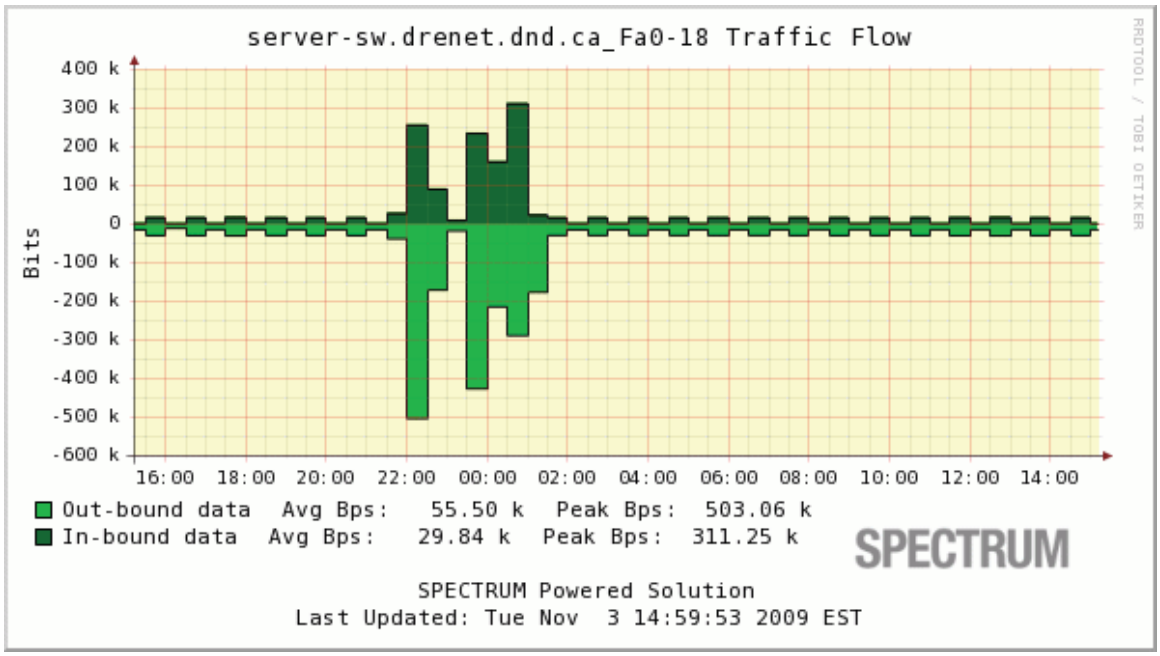

Figure 6: IP360 Bandwidth Utilization over a 24 hour period

The JNDMS integration server brokers all information transfers from DREnet systems into JNDMS. This information includes Intrusion Detection System (IDS) alerts, network and system availability alarms generated by CA Spectrum as well as vulnerability data generated by IP360. The following graph in Figure 7 shows the typical bandwidth utilized by the JNDMS Integration server system within a 24 hour period. The spike that appears at 22:00 ET is attributed with the transfer of vulnerability data generated by the IP360 system.

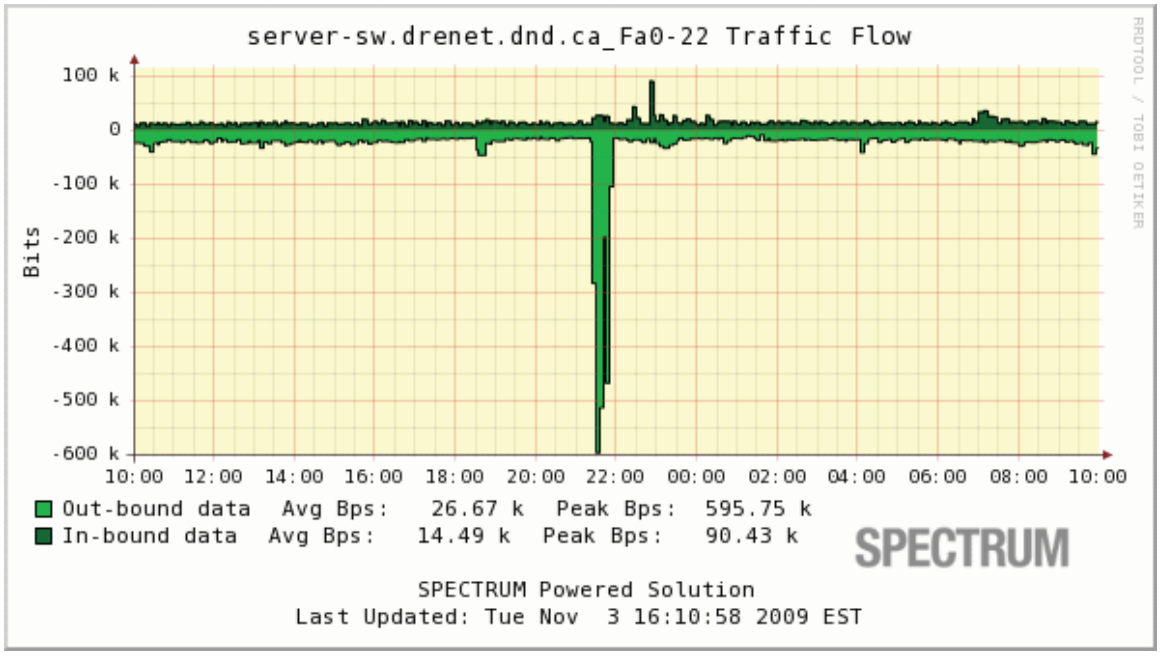

Figure 7: JNDMS Integration Server Bandwidth Utilization over a 24 hour period

The implementation of procedures to ensure that these actions occur as infrequently as is practical and attempting to schedule network discovery and scans during off hours will dramatically decrease the chance that the JNDMS will be viewed as impacting the network's throughput capability.

Another important activity for the operational implementation of a JNDMS will be to ensure the configuration and usage of network intensive COTS is done effectively in the development and test environments prior to the deployment of these tools to operational networks. As new products that compliment the JNDMS become available, this process will need to be repeated at various times throughout the system's life-cycle.

5.3.2 Scalability

The current JNDMS was built to scale to the DREnet deployment. The scope of this installation saw the JNDMS monitor approximately 130k actual assets consisting of: 3264 hosts, 473 network devices, 27 routers and 10 firewalls. Additionally the deployment included a simulated data set consisting of 216k assets. The size of a DND deployment that monitors both the CSNI and DWAN assets would be an order of magnitude beyond this. In order for a Transition to Operations project to result in a system that performs within the expectations of a modern IM application a number of efforts need to occur:

- The Decision Support System (DSS) must be able to scale its analysis capability to accommodate a much larger flow of data. This could be accomplished with effort to improve the algorithms that produce the Defensive Posture risk assessment and by expanding the hardware profile to allow for the distribution of the analysis processing across multiple CPUs invoking parallel processing.
- The Data Warehouse schema should be reviewed with the goal of query optimization. This could include how secondary assets are stored, the creation of indexes or the use of views.
- The JSS would have to be updated to ensure that data model updates could be maintained under increased load. This is another candidate for using updated hardware or distributing its load.
- Each of the input subsystems, such as Intellitactics and Spectrum, would have to be configured to scale. This would include updates to the interfaces to JNDMS in certain circumstances.
- Filtering of software assets from the Centennial application should be developed. There are a lot of very minor software tools, such as fonts, that are reported separately. These should not generally be shown to the user. One option may be to have another class of software that is not generally displayed in the User Interface but still recorded.
- All scalability efforts would have to ensure that the end user's experience remain responsive.

MDA has many years experience in the development of systems that manage high volumes of data with significant data processing requirements similar in scale to JNDMS. During the deployment of the JNDMS to the DREnet, our IPT was able to discover and resolve many issues related to the scalability of the JNDMS to a large, complex network environment. We have estimated that a reasonable minimal number of days of engineering effort are required to achieve the scalability described above. The effort is further described in the Deployment Strategy Section of this report.

5.3.3 Stability

Any full deployment would require an updated testing regime that could test all aspects of the system under full load. The stability of the system will only improve if the development and testing environment for the system allow for the conduct of testing that loads the system in the same manner that it would encounter in full operational deployment. This would require a powerful network simulation capability which is described in the Testing Considerations section of this Document. In this way, general bug fixes and component upgrades in the development and test environments should perform very closely to that of the operational system in contributing to increased stability.

5.3.4 Improved workflows

During demonstrations and experiments with the Technology Demonstrator, the IPT noted that some user workflows could be implemented as single click options within the current interface. Some effort in the design phase of the Transition to Operations Project to identify common and improved workflows could accomplish this, and then single-click links or automated reports could be implemented into the system and result in a more positive user experience.

5.3.5 Analysis Tuning

As previously mentioned, the analysis algorithms should be reviewed as the system scales to ensure that it maintains relevance and to examine better ways to express the Defensive Posture. Some possible options include:

- The implementation of a rules engine could be investigated again. The rules engines reviewed during the Technology Demonstration required significant amounts of data to prove their worth and it was found that they were better utilized in conjunction with other programming models instead of stand alone implementations. It is still believed however that rules engines could provide key benefits in allowing the system to adapt to changing environments or threats and they could also allow operators more control over the analysis. In either case having the system fully deployed and measuring the events would be essential.
- Updates to the algorithms to allow the DSS to be distributed over multiple processors would increase the performance of the risk assessment calculations. For the current deployment on the DREnet, the single processor version of the DSS takes less than 15 minutes to process the data gathered for approximately 130k assets.
- The provision of the appropriate controls to allow the operators to tune the analysis process may prove beneficial and in some cases, increase the performance of the DSS.
- Examine the possibility of having multiple, parallel, analysis engines. It has been noted that different audiences view risk and impact in different ways. The existing filters allow the focus of the operators to change, but the underlying risk remains constant for all users.
- During the period that the system is in service, the impact of new threats should be reviewed and the analysis updated to reflect new environments.
- There are a number of special cases noted during the final phases on how certain data relationships are expressed. Part of the updates to the analysis would be to ensure that whatever combination the user expresses in the portal would be addressed appropriately.

5.3.6 Mapping View Updates

The implementation of the Google Earth Web Tool Kit was demonstrated to be very beneficial to the overall usability and performance of the JNDMS. This should be integrated into JNDMS through the use of Google Enterprise Server so that there are no issues with license keys or Internet connectivity.

Google Maps should be investigated as a possibility for implementing the 2D API. The current Openlayers implementation has shown that we are pushing the system to the limits. There is a newer version of Openlayers available; however it is felt that any significant updates to the system would be best served by a migration towards Google Maps. Google is already used for the demonstration of the 3D maps and this would provide added consistency as well as the improved feature set of the Google Maps API and see a significant performance increase for that particular view.

The geographical views have shown to be beneficial and it would help the overall interface if there was more interaction with the map through the portal. This could include options such as drawing a polygon on the map and having a search done within this area. This option may require either the GIS extensions to Oracle or other database tools such as PostGIS.

6 Deployment Strategy

6.1 Overview

The JNDMS Technology Demonstration has achieved the objectives of the project to demonstrate the possibility and feasibility of Situational Awareness for Computer Network Defence for the Canadian Forces.

The gap between the concept and implementation of a fully operational JNDMS has been significantly narrowed, but as with any system as complex as the JNDMS, a sizeable effort is required to bring the system to an operational, maintainable state. The project has been executed with a strong focus on sound engineering practices and reduction of the risks associated with operational deployment.

This section will describe the anticipated effort and cost of such an endeavour using all of the information available at the time of this writing.

6.2 Resource Plan

The Section will describe the resources required to transition the JNDMS to operations. It is anticipated that in such a project that DND personnel will form the IPT with a team made up of industry professionals. For the purposes of this report, only the services/requirements for which industry would be expected to fulfill will be presented.

Table 2 presents the make up of the team required to execute the JNDMS Implementation project. The table also describes the required effort from each team resource across each of the anticipated project phases. It is important to note that the Integrated Logistics Support describes the effort of the required team members for a one year period. It is anticipated that these efforts would be required for the each of the Operational System Life-Cycle. Typically Information System Support would be expected to remain in place for a minimum of 5 years assuming the implementation is successful and usage of the system is operationally required for that period of time.

Table 2: Resource Plan

Resource Description	Project Phase				
	Project Definition	Development	Test & Integration	Training	ILS
Project Manager	12	18	12	6	25
Project Engineer	65	98	64	32	25
Project Accountant	14	20	14	8	40
Database Architect	20	40	20		
Technical Architect	10	31	20	10	
Senior Software Engineer	4	8	4	2	12
Database Developer	81	123	80	40	246
Software Engineer	81	123	80	40	
Software Engineer	4	8	4	2	12
Software Engineer	81	123	80	40	246
Test Engineer		123	80		123
Network Support	10	20	40	10	5
Quality Assurance	16	25	16	8	25
Data Management	10	10	5	10	
Contract Management	10	5	5	5	5
Procurement	5	5	5	5	5
Network Architect	10	10	5		
Information Security Analyst	81	123	80	40	25
IT Security SME	10	10			
Information Security Analyst			60		
Enterprise Information Management Architect	10	10			
Network Enterprise Management SME	5				
Network Enterprise Management Specialist	10	20			

6.3 High Level Work Plan

The Transition to Operations of the JNDMS can be captured in a high level work plan that segregates the efforts into discrete, logical phases. The following will briefly describe the phases and the activities that must occur for a successful deployment. Upon successful completion of the Project Requirements Analysis activities, this plan will require the addition of more detail to ensure that the work can be properly managed.

6.3.1 Project Definition Phase

This phase will evaluate the project as it stands and the end of the TD, including the submitted Transition Plan. This phase may build upon the System Definition and Project Management Documentation that was developed under the Technology Demonstration, but must also include discussion on the updated scope of the deployment (at the time of project initiation), the addition of derived business processes that must be in place as well as document any additional requirements that may be required at the time of the operational implementation.

6.3.2 Development Phase

The Development Phase is required to complete any development that is required to take the JNDMS from an advanced Technology Demonstration to a deployable system that scales to the operational network environment and is robust and stable in that environment. A number of development tasks will be uncovered as a result of the Project Definition Phase, but a number of development priorities are known as of the date of this writing and will need to be a part of the development plan. The majority of these development tasks are related to system performance and are described in the Performance Considerations Section (5.3) of this document. The following tasks must also be considered as part of the development phase:

- The Visualization Applet requires updating so that the layouts scale better and the more focused workflows are integrated into the applet.
- General updates to the portal should include:
  - The ability to add or edit more relationships.
  - More robust general testing.
  - Direct links to external tools. Many of the tools that act as system inputs to the JNDMS provide a web interface that could be leveraged if we knew an asset's IP address, for example.
  - Updates to the user input forms to allow faster inputs of common data.
  - Updates to the available filter and searches to support common queries and to include additional user tools such as the ability to highlight a subset of a search.
  - Update to the Google Web Toolkit portal to ensure all developed functionality is available.
- General updates to the core inputs should include:
  - The vulnerability definitions and possibly other schemas should be updated to employ the most current version.
  - Examination of additional sources of data and how they would be imported into JNDMS.
  - Updates to the firewall processing rules to support more platforms and provide more information to the JNDMS Operators.

The development phase will also contain ongoing development of integration test plans that focus not only of testing the System for stability and functionality, but that also provide proof of the System Security Baseline, which aligns the testing of the system with the required DND Certification & Accreditation processes.

6.3.3 Test and Integration Phase

The Test and Integration Phase will commence at the close of development with the system Configuration Managed for controlled builds to the test environment designated for deployment. All tests will be executed, identified deficiencies will be remedied or deemed acceptable, and the build and testing will continue to cycle until the system is ready for deployment.

The integration activities will commence with the development of a comprehensive deployment plan which maps out the details of the deployment, including stakeholder management.

The Test Design Documentation and the DREnet deployment Plan developed under the JNDMS Technology Demonstration should be referenced to aid in the planning of this phase.

6.3.4 Training Phase

The Training Phase of the project will ensure that all User Guide and Training Materials are complete and will conclude with both Classroom and "on the job" training sessions for the required JNDMS user personnel. In addition to the initial training sessions, part of the ILS phase will be to repeat the training sessions as replacement staff are assigned during the system's operational life-cycle.

6.3.5 Integrated Logistics Support Phase

The ILS Phase of the project will provide the ongoing support required to keep the system operational, current and meeting its stated operational objectives for the duration of the system life-cycle.

Further detail on the ILS plan for the JNDMS is provided in Section 7 of this document.

6.4 Schedule

The duration of the JNDMS Implementation is currently planned to be 16 months from project kick-off and running up to the initial one year ILS term. Table 3 describes the anticipated duration of each phase of the project. A high-level schedule may be found in Figure 8. The start and end dates are assumed and only applicable to this report.

Table 3: Project Phase Duration

Phase	Months
PD	4
Development	6
Integration	4
Training	2
ILS	Yearly

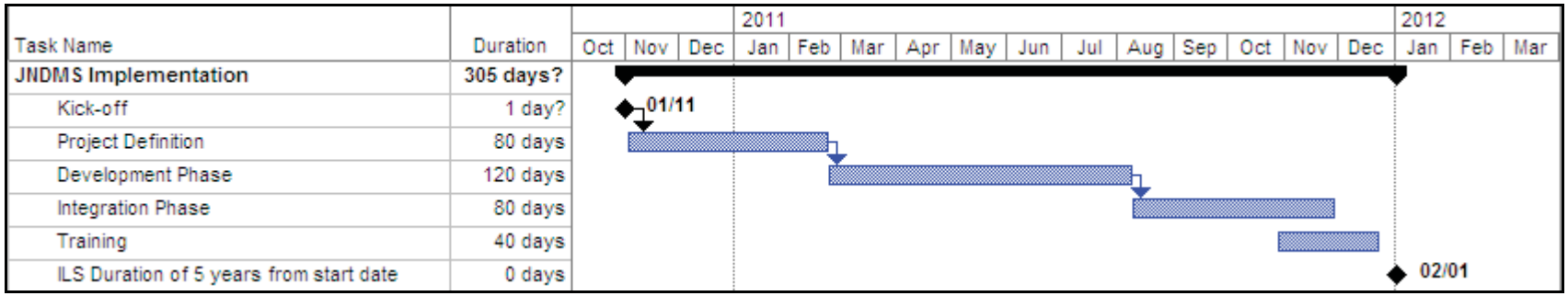

Figure 8: JNDMS Implementation Schedule

This Page Intentionally Left Blank

6.5 Budget/Cost

The financial numbers provided in this section represent working numbers only to provide DND with a starting point for Options Analysis and Requirements Analysis from which to Budget for an actual JNDMS Implementation Project. The values provided for this purpose in no way represent an offer of cost to sell, rough order of magnitude pricing or estimate of cost from MacDonald Dettwiler to the Crown. The labour effort and per diem rates are a representation only of typical standard industry rates for the category of Defence & Security IT professionals at the time of this writing. The purchased equipment and COTS product costs are based on informal quotations that certainly represent the costs expected for the scope of deployment described in this plan, but must be expected to change over time until such products are actually procured. Also, between the time of this writing and the actual project procurements, DND may either have purchased one or more of the COTS products or comparable products outside the scope of the project, eliminating them from project costs.

6.6 Scope

For the purposes of this report, the cost of the JNDMS Implementation includes the cost of the effort to bring the JNDMS system to an operational state and the cost of deploying and supporting the operational system for one year following the deployment. Additional years of support are expected to incur similar costs as the first, as is typical with IT system In Service Support efforts. It is important to note that only projected costs of the anticipated operational system are included here. The cost of further redundant systems and systems for performing data backups are not part of this budgeting effort.

The JNDMS System costs described herein are limited to the following:

- 2 JNDMS installations on the CSNI.
- 1 JNDMS installation on the DWAN configured for data forwarding to the CSNI JNDMS systems.

Table 4 describes each the recommended COTS products to be included in the implementation of the JNDMS subsystems. Where possible, the table indicates if the product requires procurement or is already part of the DND Network Infrastructure. Certain products are listed as future requirements and are not included in the costs at this time.

This Page Intentionally Left Blank

Table 4: JNDMS COTS

Subsystem	Service	Final Configuration	Required?	Comment
Security Infrastructure Mgmt				
	SIM core	ISM	Required	Assume existing infrastructure
	Vulnerability Management	IP360	Required	Assume existing infrastructure
	Policy Violations		Future	Possible, requires updates, no use so far
JNDMS User Interface				
	Portal	Tomcat	Required	
	Mapping	Google Enterprise	Required	Assume existing infrastructure
	Client	IE / Firefox	Required	
	GWT		Required	
	ExtJS		Required	Code licenses required, not run time
Enterprise Infrastructure Mgmt				
	Unicenter NSM / EIM Core	Spectrum	Required	
	Asset management	Centennial	Required	Assume existing infrastructure
	CMDB (RFC management)		Future	
	Performance Monitoring	eHealth	Optional	
	Topology	[Spectrum]	Required	
	Topology / Com links	NTSM	Optional	
	Fault Monitoring / Alerts	[Spectrum]	Required	
	Faults / Tickets	ESMS	Optional	DND tool
	Service management (TBD)	N/A	Future	
JNDMS System Services				
	Application Server	Tomcat	Required	
	Data transformations		N/A	Internal tools used
Decision Support System				
	DSS	Java	Required	Code licenses required, not run time (Jgraph, JEP)
	DSS Extensions	Aion (Rules), Analysis	Future	Experiment with adaptive technology
JNDMS Data Warehouse				
	Data warehouse	Oracle	Required	

This Page Intentionally Left Blank

Table 5 provides the cost derived from the Resource Plan in Section 6.2 of this document and the estimates for the COTS products and other purchased equipment.

Table 5: Pricing by Project Phase

Item	Project Definition	Development	Integration	Training	Implementation Total	ILS
Base System Labour	$790,413	$1,414,590	$604,338	$340,810	**$3,150,152**	$972,748
Base Purchased Equipment		$28,930	$0		**$28,930**	$7,068
Labour CSNI			$604,338		**$604,338**	
Labour DWAN			$604,338		**$604,338**	
Purchased Equipment CSNI	$0		$454,373	$0	**$454,373**	$101,663
Purchased Equipment DWAN			$227,186		**$227,186**	$50,832
Computer Associates Products CSNI	$0		$1,473,835	$0	**$1,473,835**	$295,928
Computer Associates DWAN			$11,024,750		**$11,024,750**	$2,204,950
CSNI Totals	**$790,413**	**$1,414,590**	**$3,136,884**	**$340,810**	**$5,682,698**	**$1,370,339**
DWAN Totals	**$790,413**	**$1,414,590**	**$12,460,613**	**$340,810**	**$15,006,426**	**$3,228,529**

6.7 Risk Plan

The Risk Plan of the JNDMS Technology Demonstration Plan should be implemented for the JNDMS Implementation Project. Risk Planning must begin very early in the project and maintained and monitored throughout the life of the project. The Risk Plan for the JNDMS Technology Demonstrator was based on MDA's proven Risk Management Process and will scale without change to the JNDMS Implementation Project. For further detail on the Risk Plan refer to the Project Management Plan for the Joint Network Defence and Management System (JNDMS) Project DID PM 001.

7 Integrated Logistics Support Strategy

7.1 Overview

The JNDMS will require Integrated Logistics Support for the operational life-cycle of the system. ILS provides the project with a team of experts to plan, track, control, and test and implement any bug fixes, system updates and enhancements that the JNDMS System may require.

7.2 Resource Plan

The resource plan for the ILS portion of the JNDMS Implementation can be found in Section 6.2 of this document. The resources and identified effort represent one year's worth of support. The effort and resources required may be revisited on a yearly basis, but the demand for evolution of an information system during its life-cycle will require similar resources and effort from year to year.

7.3 High Level Work Plan

The ILS team is responsible for ensuring that the JNDMS System is properly configuration managed and that issues raised by DND are tracked, resolved and integrated into the operational system through managed builds. The team is also responsible for the development of a plan that sees system testing developed and guidance and assistance is provided to DND in the execution of all system integration tests.

All development performed by the ILS team must adhere to the System Engineering and Software Engineering Plans developed during the Project Definition Phase of the project.

Finally, it may be desired by DND, that the ILS project team manage the maintenance support efforts for any of the COTS systems that act as system inputs for the JNDMS.

7.4 Schedule

Schedule of activities for an ILS project are typically driven by the priority of issue resolution set by the Operational and Technical authorities for the system. The schedule of activities leading up to an updated build to the production environment would be developed once those priorities are identified.

7.5 Budget/Cost

The Budget and Cost of ILS support for the JNDMS Implementation is highlighted in Section 0 of this document. The costs associated with ILS support do not include Maintenance Agreements for the COTS that JNDMS is required to interface with. Those costs are included in the product purchase costs of the project.

7.6 Risk Plan

The Risk Management Plan for an ILS project does not differ from that of a development and integration project. Please refer to Section 6.7 of this document.

8 System Testing Considerations

The Test Design Document For The Technology Demonstration Of The Joint Network Defence and Management System (JNDMS) Project DID SD 003 provides a comprehensive description of the type of testing required to validate the JNDMS for functionality, including validation of the interfaces with the external systems (COTS) employed during the life of the project. This was sufficient for a Technology Demonstration project, but requires further consideration and effort to scale the testing plan and design to meet the requirements of a JNDMS Implementation Project. In order to meet this need, the Resource Plan and cost estimates for the Development, Test and Integration Phases of the project contain additional effort for the enhancement of the testing plan and design, as well as, the execution of all anticipated tests.

There are a number of areas in which testing must be augmented in the evolution of the JNDMS TD to a fully deployed operational system:

- Tests must be developed to validate the interface and transformation of data from any new system inputs that have to date not been included in the JNDMS. This includes any interfaces to new Network or Security Management COTS purchased by DND or interfaces to existing DND tools or systems that have previously not been interfaced by the JNDMS.
- Scalability testing for the magnitude of the CSNI and DWAN networks. During the life of the Technology Demonstration, the scalability of the system grew to the level of capability required for a fully operational deployment on the DREnet. In order to meet acceptable performance requirements for DND's operational networks, a powerful simulation capability must be implemented in the JNDMS development and test environments so that the system scalability may be validated prior to deployment.
- General user interface testing. In the final configuration of the JNDMS User Interface, the Google Earth Web Toolkit portal technology was developed and resulted in dramatic improvements to the performance and usability of the application. Time for testing the new interface was limited and will require that the UI test plans received significant effort to ensure that the application is robust and provides a positive user experience.
- The final consideration for the enhancement of testing of the JNDMS towards an operational employment is in the area of System Security Tests. The Statement of Sensitivity for the JNDMS Implementation will show that in order to obtain the necessary DND Security Certification and Accreditation, the JNDMS must implement several layers of security and system testing must align with the expectations of the C&A process.

It should be noted that the acquisition of a robust and powerful network simulation environment for the development and test environments will aid in providing the capability to validate the JNDMS performance with a scope and flow of data that would closely replicate that of a DND Operational network. Although not costed in this plan, industry leading companies such as OPNET offer solutions that should be considered for any Information System Project that interface with large networks and high throughputs of data.

9 Success Factors

The success of a transition to operations of the JNDMS will rely heavily on understanding mitigating any outstanding challenges issues that affect the scope, level of difficulty and feasibility of this plan. We have categorized these issues into challenges, assumptions and proposed solutions.

9.1 Technical Challenges

The majority of the technical challenges that remain and the proposed solutions required to close the gap between the JNDMS Technology Demonstration and an operationally deployed JNDMS have been documented throughout this document (Sections 17 Performance Considerations and 6.3.2 which describes the development strategy).

However, it is worth re-iterating the key technical hurdles that require resolution prior to a successful operational deployment of the JNDMS:

- Scalability for processing capability and bandwidth control is a key concern and must be addressed, including the capability to simulate the scope of DND operational networks in the development and test environments.
- Performance of the Decision Support System both in processing ability and functions to provide user tuneable decisions.
- Improvements to the performance of the User Interface including updates to the mapping views and the identification and implementation of an improved user workflow.

9.2 Programmatic Challenges

Many programmatic challenges have been mitigated over the duration of the JNDMS Technology Demonstration, particularly during the task involving the deployment to the DREnet network. Engagement with all major stakeholders early and often, as well as, being very open and flexible when working with Network and IT Security managers will be key to the success of any future JNDMS endeavours. There still, however remain a few very large challenges ahead when considering an operational deployment of a JNDMS capability.

Situational Awareness for Computer Network Defence and the value of Computer Network Defensive Posture are still very new concepts to the Canadian Forces Operational Commanders. Although much attention in the media is now focused on the threat of cyber-attacks on military networks, it is still not necessarily viewed as a crucial capability. Demonstrations provided as part of the JNDMS project have certainly raised awareness of this, but the buy-in commitment from the Canadian Forces at the highest levels is still one of the most significant challenges to the success of an operationally deployed JNDMS.

Secondly, a significant cultural change is required of Network and IT Security managers and teams across the many DND installations nation-wide, before the JNDMS will be able to provide truly meaningful SA for CND. In order to do this, the JNDMS requires a significant amount of information from many network enclaves and the assurance that the information is complete, regularly maintained and made available by network and system owners.

Finally, the JNDMS concept relies heavily on the ability to provide SA for CND in the context of specific military operations. Currently the standards and capability for operational commanders to provide this data in a consistent and complete manner is in the infancy stages. The JNDMS currently provides user-entered forms for this process, but without an enforceable standard, it is very difficult to produce a consistent risk/impact assessment that is of value to the command and control of military operations.

The solution to all of these challenges lies in the ability to openly engage stakeholders early and often during a JNDMS Implementation Project.

9.3 Assumptions

The following list of assumptions was made in the preparation of the estimates contained in this plan. These assumptions must be either mitigated or validated prior to the transition of the system.

- CSNI can be maintained with two JNDMS installations. A third JNDMS would be required to provide way data feeds from the DWAN to the CSNI.
- One way data feeds are available and can pass JNDMS data (generally xml formatted)
- Estimates assumes that IP360 and Intellitactics are fully deployed on both the CSNI and DWAN
- Projects cover core requirements of JNDMS
- The quoted servers are sufficient for scalability (scalability studies to be done)
- The TD will meet all core requirements at the end of development.
- Assume all development support and licenses from TD are still valid
- Assume ISM licenses already purchased and deployed
- nCircle IP360 / MCPS / Deepsight covered by DND
- MCPS covered by DND
- Assumes 5 CACLS will be sufficient for Windows 2003 server, additional covered by DND
- Assumes backups, system administration and server maintenance/replacement covered by DND
- DSS not required on feeder JNDMS
- Aion BRE option is not included
- Oracle licenses based on 6 processors over three systems
- Assumption that Google Earth Enterprise Licenses already owned by DND will be available to the project
- Assume Centennial has been deployed

Annex A Product Basis of Estimate

Table 6: Product Basis of Estimate

Subsystem	Service	Dev Only	1 System	Dev Maint.	1 Sys. Maint	Config/Product	Required	Notes/Assumptions
SIM								
	SIM core		$0	$0	$0	ISM	Required	Assume existing infrastructure
	Vulnerability Management		$0	$0	$0	IP60	Required	Assume existing infrastructure
	Policy Violations		$0	$0	$0		Future	Not included
JUI			$0	$0	$0			
	Portal	$2,400	$5,760	$0	$18,000	Tomcat	Required	Tomcat support services
	Mapping		$0	$0	$0	Google Enterprise	Required	Assume existing infrastructure
	Client		$0	$0	$0	IE / Firefox	Required	Common / free tools
	GWT	$0	$0	$0	$0		Required	
	ExtGWT	$2,640	$0	$1,200	$0		Required	Code licenses required, not run time. Maintenance included.
EIM			$0	$0	$0			
	Unicenter NSM / EIM Core		$0	$0	$0	Spectrum	Required	Costs covered in CA products
	Asset management		$0	$0	$0	Centennial	Required	Assume existing infrastructure
	CMDB (RFC management)		$0	$0	$0		Future	Not included
	Performance Monitoring		$0	$0	$0	eHealth	Optional	Not included
	Topology		$0	$0	$0	Spectrum	Required	Costs covered in CA products
	Topology / Com links		$0	$0	$0	NTSM	Optional	Not included
	Fault Monitoring / Alerts		$0	$0	$0	Spectrum	Required	Costs covered in CA products
	Faults / Tickets		$0	$0	$0	ESMS	Optional	Not included
	Service management (TBD)		$0	$0	$0	N/A	Future	Not included
JSS			$0	$0	$0			
	Application Server		$0	$0	$0	Tomcat	Required	Tool is at no cost, services included as part of portal (also Tomcat)
	Data transformations		$0	$0	$0		N/A	
DSS			$0	$0	$0			
	DSS	$6,000	$0	$1,440		Java	Required	Code licenses and maintenance required (Jgraph, JEP), not run time. Aion BRE not included
	DSS Extensions		$0	$0	$0	Aion (Rules), Analysis	Future	Not included
JDW			$0	$0	$0			
	Data warehouse		$113,327	$0	$22,665	Oracle	Required	Price from website for 4 processors + 2 processors on DWAN. Maintenance was estimated at 20%
	General Dev support	$10,000		$2,500	$0			

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

API	Application Programmer Interface
C&A	Certification & Accreditation
CACLS	Change Access Control Lists
CF	Canadian Forces
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Centre
CIRT	Cyber Incident Response Team
COMPUSEC	Computer Security
CND	Computer Network Defence
ConOps	Concept of Operations
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off The Shelf
CSNI	Canadian Secret Network Infrastructure
CWID	Coalition Warrior Interoperability Demonstrations
DND	Department of National Defence
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
DREnet	Defence Research Experimental Network

DSS	Decision Support System. Part of JNDMS
DWAN	Defence Wide Area Network
EIM	Enterprise Information Management. Part of JNDMS
ESMS	Enterprise Support Management System
GIS	Geographical Information System
GWT	Google Web Toolkit
HTRAM	Harmonised Threat Risk Assessment Methodology
IAT	Impact Assessment Tool
IDS	Intrusion Detection System
ILS	Integrated Logistics Support
IPSEC	Secure Internet Profile
IPT	Integrated Project Team
ISM	Intellitactics Security Manager
ITIL	Information Technology Infrastructure Library
ITSE	Information Technology Security
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JDW	JNDMS Data Warehouse
JNDMS	Joint Network and Defence Management System

JSS	JNDMS System Services
LAN	Local Area Network
MDA	MDA Systems Ltd.
NTSM	National Telecommunications System Manager
ODBC	Open Database Connectivity
OGD	Other Government Department
PKI	Public Key Infrastructure
POC	Proof of Concept
RCMP	Royal Canadian Mounted Police
RDBMS	Relational Database Management System
RFC	Request For Change
R&D	Research & Development
SA	Situational Awareness
SIM	Security Information Management. Part of JNDMS
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures
SQL	Structured Query Language
SSL	Secure Socket Layer

TRA	Threat Risk Assessment
UI	User Interface
XML	Extensible Mark-up Language

This Page Intentionally Left Blank